UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,487	03/18/2005	Pim Theo Tuyls	NL 020950	6387

24737 7590 03/31/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
4193	

MAIL DATE	DELIVERY MODE
03/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/528,487	TUYLS ET AL.	
	Examiner	Art Unit	
	DARREN B. SCHWARTZ	4193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10-12-06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because the applicant refers to "Diffie-Hellmann" (line 5). This should be changed to "Diffie-Hellman." Correction is required. See MPEP § 608.01(b).

2. The disclosure is objected to because of the following informalities: The applicant refers repeatedly in the specification to "Diffie-Hellmann" (see page 3, line 19, 25, 31, etc). This should be changed to "Diffie-Hellman."

Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 16 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 16 is directed to software, *per se*. The body of the claim is directed a program itself, that is, descriptive material per se, non-functional descriptive material, and is not statutory because it is not a physical "thing" nor a statutory process. Such claims do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program's functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process without the computer-readable medium needed to realize the computer

program's functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program's functionality to be realized, and is thus statutory. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

Claim Objections

5. Claim 6 is objected to because of the following informalities: Reference is made user facility 1 and user facility 2 on page 9, lines 27-28. Claim 1, upon which claim 6 depends, recites user facility i and user facility j on page 9, line 2. Appropriate correction is required.

6. Claim 15, line 1, recites "and/or" and renders the claim indefinite. This should be changed to "and" or "or." Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 4-6, 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 4, line 18 recites the limitation, "$S_i = f_T(r_i)$ and $P_i=g(r_i)$. It is unclear as to what function f_T does; the specification merely cites the mathematical representation on

page 7, line 31. It is unclear as to the meets and bounds of the claim with respect to said functions.

Claims 4, line 18 recites a variable r_i. It is unclear as to what r_i represents. While the applicant discloses a point r in Z_q. It has not been established in the claim as to the meets and bounds of the variable.

Claim 5, variables s_{i1}, s_{i2}, p_{i1}, p_{i2}, T_{11}, T_{12}, T_{21}, T_{22} are not defined in the claim nor the claims upon which it depends.

Claim 6 recites several data recited on page 9, line 29 and page 10, lines 1-7. The Diffie-Hellman triple data recite variables and formulas that have not been defined.

Claim 9 recites the limitation "the Weil Pairing." It is unclear as to what is evaluated and how this further limits the parent claim. Claim 9 further recites "the protocol proper." All the limitations of claim 1 recite a method; as such, it is a series of steps or protocols that describe one's invention. Since the series of steps or protocols of claim 1 cannot be reordered, it is unclear as to where the "Weil Pairing is evaluated" in claim 1.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-3, 8, 9 and 11-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon (U.S. Pat Pub 2002/0129247 A1), hereinafter referred to as

Jablon, in view of Joux, Antoine, "A One Round Protocol for Tripartite Diffie-Hellman," hereinafter referred to as Joux.

Re claim 1: Jablon teaches a method for generating a common secret data item between a first user facility i and a second user facility j (Abstract: lines 11-13) through by each such user facility executing mutually symmetric operations [Fig 1: steps 101, 102, 103, 104 coincide with steps 121, 122, 123, 124] on respective complementary data items (¶66) that are based on respectively unique quantities (Fig 1, elts 101, 121 & 102, 122) and that are at least in part secret (¶66, lines 1-3: shared secret S), and wherein an outcome of said operations is used in both said user facilities as said common secret data item (page 4, left column 2: lists 1 and 2 and ¶67-¶69; generate key K).

However, Jablon is silent as to said method being characterized in being based on defining said complementary data belonging to a GAP Diffie-Hellmann Problem that is defined in an Abelian Variety.

Joux teaches said method being characterized in being based on defining said complementary data belonging to a GAP Diffie-Hellmann Problem [variation of the Diffie-Hellman protocol] that is defined in an Abelian Variety (Abstract).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the Jablon reference to teach a computationally difficult math problem which uses Elliptic curves, a particular Abelian Variety, as taught by Joux, for the purpose of providing a computationally difficult problem for the basis of a key exchange and a secure communication exchange.

Re claim 2: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Official notice is taken as to the limitation said Abelian Variety has a dimension one through being an elliptic curve. It is known in the art that an abelian variety is an algebraic group which is a complete algebraic variety. An Abelian variety of dimension 1 **is** an elliptic curve.

Re claim 3: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux further teach applying a pairing F featuring a bilinearity property, a non-degeneration property, and a computability property to two linearly independent points P and D(P) on said Abelian Variety (Joux: page 1, line 7-8; specifically Weil pairing).

Re claim 8: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux further teach the generating of such shared secret is used as an initial step in an identification or authentication procedure (Jablon: Fig 1, elt 127; ¶73 and ¶76).

Re claim 9: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux further teach the Well Pairing is evaluated at an instant in time that lies substantially before executing the protocol proper (Joux: page 1, lines 7-8).

Re claim 11: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux further teach the method of being executed through using only a single integrated cryptography level (Jablon: Fig 1, elt

101 & 121: there is only one secret data established and Fig 1, elt 127: there is only one verification routine).

Re claim 12: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux further teach a randomization scheme is applied to the common secret (Jablon: Fig 1, elts 103 & 123; ¶66, ¶67 and page 4, left column, lists 1 & 2).

Re claim 13: Jablon in view of Joux teach all the limitations of claim 13 as previously discussed. Jablon in view of Joux further teach the randomization scheme is based on a challenge-response mechanism (Jablon: Fig 4, all elts).

Re claim 14: Jablon in view of Joux teach a system comprising a first user facility [Alice] and a second user facility [Bob], and being arranged to communicate according to the method as claimed in Claim 1 (Jablon: Fig 1, elts 100 & 120) (see claim 1 above).

Re claim 15: Jablon in view of Joux teach a device being arranged to operate as the first and/or second user facility in a system (Jablon: ¶11) as claimed in Claim 14 (see claim 14).

Re claim 16: Jablon in view of Joux teach a computer program product comprising instructions for controlling one or more data processing oriented hardware entities (Jablon: ¶11 & ¶322) to implement a method as claimed in Claim 1 (see claim 1).

11. Claims 7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jablon (U.S. Pat Pub 2002/0129247 A1), hereinafter referred to as Jablon, in view of

Joux, Antoine, "A One Round Protocol for Tripartite Diffie-Hellman," hereinafter referred to as Joux, in further view of Menezes et al., "Handbook of Applied Cryptography," hereinafter referred to as Menezes.

Re claim 7: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux do not teach a revocation scheme on top of its standard scheme for excluding one or more selected user facilities through assigning to every user facility its own unique parameters.

Menezes teaches a revocation scheme on top of its standard scheme for excluding one or more selected user facilities through assigning to every user facility its own unique parameters (page 576-577, section 13.6.3; specifically "certification revocation" and steps 1-5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the combination of Jablon and Joux reference to invoke a key revocation scheme, as taught by Menezes, for the purpose of preventing subsequent use of or trust in the associated keying material.

Re claim 10: Jablon in view of Joux teach all the limitations of claim 1 as previously discussed. Jablon in view of Joux do not teach updating of secret information against divulgation of an earlier secret information.

Menezes teaches comprising an updating of secret information against divulgation of an earlier secret information (page 579, Fig 13.10).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the combination of Jablon and Joux reference to

invoke a key update scheme, as taught by Menezes, for the purpose of protecting keys and their storage (see Menezes: page 578).

Conclusion

12. Because the claims are rendered indefinite by the several issues detailed above in reference to the rejection under 35 U.S.C. 112, second paragraph, it has not been possible to determine the scope of the claims, and therefore it has not been possible to fully search the prior art for the claimed subject matter in order to make a determination regarding the patentability of the claims with respect to novelty under 35 U.S.C. 102 and non-obviousness under 35 U.S.C. 103. A search has been made to the extent possible, and documents which appear to be relevant are cited.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Darren B. Schwartz whose telephone number is 571-270-3850. The examiner can normally be reached on Monday-Friday 8:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Long Nguyen can be reached on 571-272-1753. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DS

/Long Nguyen/
Supervisory Patent Examiner
Art Unit 4193